

ORIGINAL



An Employee Owned Company
3027 Stokley Street
Philadelphia, Pennsylvania 19129-1188
215-844-6600

January 11, 1994

RECEIVED

JAN 14 1994

FCC MAIL ROOM

Mr. William F. Canton,
Acting Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, DC 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning toll fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPR vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXC's, LEC's and CPE's, the law should reflect that. It is preposterous to think that the IXC's, LEC's and CPE's who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPE's should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPE's ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installations of the equipment with the customers full knowledge. CPE's should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

No. of Copies rec'd
List A B C D E

Orig

Striving for Excellence In our Second Century



WALTON, MA (BOSTON) 02154 W. SPRINGFIELD, MA 01089 PLAINVIEW, N.Y. 11803 PHILADELPHIA, PA. 19129
PITTSBURGH, PA. 15222 READING, PA. 19601 PENNSAUKEN, N.J. 08109 BALTIMORE, MD. 21209 SPRINGFIELD, VA. 22153
JACKSONVILLE, FL. 32204 ORLANDO, FL. 32803 MIAMI, FL. 33125



William F. Canton
January 11, 1994
Page Two

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Spring Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addressed the symptom of the problem of toll fraud and not the cause.

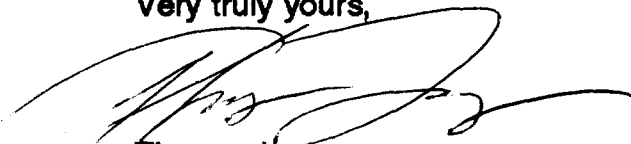
The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

William F. Canton
January 11, 1994
Page Three

Toll Fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Thomas Logue', with a large, sweeping flourish extending to the right.

Thomas Logue,
Telecommunications Manager

TL/sn